[19]中华人民共和国国家知识产权局

[51]Int. Cl⁷ H04L 9/32

D2

[12]发明专利申请公开说明书

[21]申请号 00808659.1

[43]公开日 2002年6月19日

[11]公开号 CN 1354936A

[22]申请日 2000.8.9 [21]申请号 00808659.1

[30]优先权

[32]2000.4.14 [33]KR [31]2000/19727

[86]国际申请 PCT/KR00/00875 2000.8.9

[87]国际公布 WO01/80482 英 2001.10.25

[85]进入国家阶段日期 2001.12.7

[71]申请人 韩国稀客股份有限公司

地址 韩国京畿道

[72]发明人 殷有进 洪起隆

李玟求 金材洛

[74]专利代理机构 北京市柳沈律师事务所

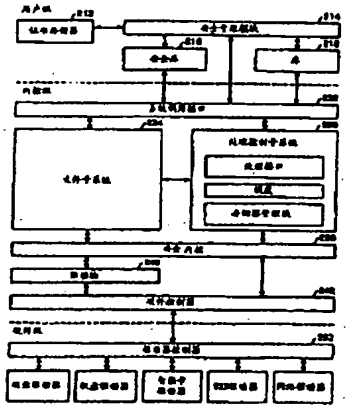
代理人 马莹 邵亚丽

权利要求书6页 说明书9页 附图页数13页

[54]发明名称 基于数字签名证书保护文件系统的方法和装置

[57]摘要

公开了一种保护文件系统的方法和装置。该保护文件系统的方法包括步骤:a)为系统安全管理员生成第一数字签名密钥和系统安全管理员的证书;b)当在服务器计算机上安装操作系统时,将系统安全管理员的证书存储到安全内核中;c)为用户生成第二数字签名密钥和用户的证书;d)设置文件系统的访问权限;e)当用户试图访问文件系统时,通过数字签名身份验证的方法识别用户;以及f)根据识别结果授予用户对文件的访问权限。



ISSN1008-4274

01.12.07

权 利 要 求 书

1. 一种保护计算机中的文件系统的方法，其中对文件具有访问权限的用户可以访问计算机中的文件系统，该方法包括步骤：

a）生成系统安全管理员的数字签名密钥和系统安全管理员的证书；

b）当在服务器计算机上安装操作系统时，将系统安全管理员的证书存储到安全内核中；

c）生成第二数字签名密钥和用户的证书；

d）设置文件系统的访问权限；

e）当用户试图访问文件系统时，通过基于数字签名的身份验证识别用户；以及

f）根据识别结果授予用户对该文件的访问权限。

2. 如权利要求 1 所述的方法，还包括步骤：g）如果将用户识别为系统安全管理员，则执行用户注册/删除处理。

3. 如权利要求 1 所述的方法，还包括步骤：h）如果将用户识别为系统安全管理员，则设置文件系统的访问权限。

4. 如权利要求 1 所述的方法，还包括步骤：i）访问并处理文件。

5. 如权利要求 1 所述的方法，其中步骤 a）包括步骤：

a-1）生成系统安全管理员的公共密钥；

a-2）生成系统安全管理员的保密密钥；和

a-3）生成系统安全管理员的证书。

6. 如权利要求 1 所述的方法，其中步骤 e）包括步骤：

e-1）在服务器计算机中生成随机数；

e-2）生成对该随机数的数字签名；

e-3）从存储在安全内核上的系统安全管理员的证书中提取系统安全管理员的公共密钥；

e-4）通过提取的系统安全管理员的公共密钥验证用户的证书；

e-5）提取用户的公共密钥和用户证书中的访问权限；和

e-6）验证对该随机数的数字签名。

7. 如权利要求 1 所述的方法，其中步骤 f）包括步骤：

f-1）如果用户是一般用户，则提供该用户对文件系统的文件系统访问权

限；和

f-2）向该用户提供注册/删除权限、文件系统访问设置权限和文件系统访问权限。

8. 如权利要求 2 所述的方法，其中步骤 g）包括步骤：

g-1）确定是否选择了用户注册或删除；

g-2）如果选择了用户删除，则删除与将要被删除的用户有关的数据；

g-3）如果选择了用户注册，则注册一个用户；

其中的步骤 g-3）包括以下步骤：

g-3-1）提供访问权限给将要注册的用户；

g-3-2）生成将要注册的用户的保密密钥和公共密钥；

g-3-3）生成将要注册的用户的证书；

g-3-4）加密并存储将要注册的用户的保密密钥；和

g-3-5）存储将要注册的用户的证书。

9. 如权利要求 8 所述的方法，其中证书是通过加密访问权限和用户的公共密钥生成的。

10. 如权利要求 3 所述的方法，其中步骤 h）包括步骤：

h-1）选择一文件；

h-2）选择允许访问该文件的用户；和

h-3）设置对该文件的访问权限为用户的访问权限。

11. 如权利要求 4 所述的方法，其中访问并处理文件的步骤 i）包括步骤：

i-1）接收将要访问的文件的名称；

i-2）确定将要访问的文件的访问权限是否等于系统安全管理员的访问权限；

i-3）如果将要访问的文件的访问权限等于系统安全管理员的访问权限，则允许该文件被访问；

i-4）确定将要访问的文件的访问权限是否等于试图对此访问的用户的访问权限；

i-5）如果将要访问的文件的访问权限等于试图对此访问的用户的访问权限，则允许该文件被访问。

12. 一种保护计算机系统中的文件系统的装置，其中对文件具有访问权限的用户可以访问计算机系统中的文件系统，该装置包括：

生成系统安全管理员的数字签名密钥和系统安全管理员的证书的部件；

当在服务器计算机上安装操作系统时，将系统安全管理员的证书存储到安全内核中的部件；

生成用户数字签名密钥和用户的证书的部件；

设置文件系统的访问权限的部件；

当用户试图访问文件系统时，通过数字签名身份验证的方法识别用户的部件；以及

根据识别结果授予用户对文件的访问权限的部件。

13. 如权利要求 12 所述的装置，还包括如果将用户识别为系统安全管理员，则执行用户注册/删除的部件。

14. 如权利要求 12 所述的装置，还包括如果将用户识别为系统安全管理员，则设置文件系统的访问权限的部件。

15. 如权利要求 12 所述的装置，还包括访问并处理文件的部件。

16. 如权利要求 12 所述的装置，其中生成系统安全管理员的数字签名密钥和系统安全管理员的证书的部件包括：

生成系统安全管理员的公共密钥的部件；

生成系统安全管理员的保密密钥的部件；和

生成系统安全管理员的证书的部件。

17. 如权利要求 12 所述的装置，其中识别用户的部件包括：

在服务器计算机中生成随机数的部件；

生成对该随机数的数字签名的部件；

从存储在安全内核上的系统安全管理员的证书中提取系统安全管理员的公共密钥的部件；

通过提取的系统安全管理员的公共密钥验证用户的证书的部件；

提取用户的公共密钥和用户证书中的访问权限的部件；和

验证对该随机数的数字签名的部件。

18. 如权利要求 12 所述的装置，其中授予用户访问权限的部件包括：

如果用户是一般用户，则给该用户提供对文件系统的文件系统访问权限的部件；和

给该用户提供注册/删除权限、文件系统访问设置权限和文件系统访问权限的部件。

19. 如权利要求 13 所述的装置，其中执行用户注册/删除步骤的部件包括：

确定是否选择了用户注册或删除的部件；

如果选择了用户删除，则删除与将要删除的用户有关的数据的部件；

如果选择了用户注册，则注册一个用户的部件；

其中注册用户的部件包括：

提供访问权限给将要注册的用户的部件；

生成将要注册的用户的保密密钥和公共密钥的部件；

生成将要注册的用户的证书的部件；

加密并存储将要注册的用户的保密密钥的部件；和

存储将要注册的用户的证书的部件。

20. 如权利要求 19 所述的装置，其中用户证书是通过加密用户的访问权限和用户的公共密钥生成的。

21. 如权利要求 14 所述的装置，其中设置访问权限的部件包括：

选择一文件的部件；

选择允许访问该文件的用户的部件；和

设置对该文件的访问权限为用户的访问权限的部件。

22. 如权利要求 15 所述的装置，其中访问并处理文件的部件包括：

接收将要访问的文件的名称的部件；

确定将要访问的文件的访问权限是否等于系统安全管理员的访问权限的部件；

如果将要访问的文件的访问权限等于系统安全管理员的访问权限，则允许该文件被访问的部件；

确定将要访问的文件的访问权限是否等于试图对此访问的用户的访问权限的部件；以及

如果将要访问的文件的访问权限等于试图对此访问的用户的访问权限，则允许该文件被访问的部件。

23. 一种存储用于执行保护计算机中文件系统的方法的指令的计算机可读介质，其中具有文件访问权限的用户可以访问计算机中的文件系统，该方法包括步骤：

a）生成系统安全管理员的数字签名密钥和系统安全管理员的证书；

b）当在服务器计算机上安装操作系统时，将系统安全管理员的证书存储到安全内核中；

c）生成第二数字签名密钥和用户的证书；

d）设置文件系统的访问权限；

e）当用户试图访问文件系统时，通过基于数字签名的身份验证识别用户；以及

f）根据识别结果授予用户对文件的访问权限。

24. 如权利要求 23 所述的计算机可读介质，其中所述方法还包括步骤：

g）如果将用户识别为系统安全管理员，则执行用户注册/删除处理。

25. 如权利要求 23 所述的计算机可读介质，其中所述方法还包括步骤：

h）如果将用户识别为系统安全管理员，则设置文件系统的访问权限。

26. 如权利要求 23 所述的计算机可读介质，其中所述方法还包括步骤：

i）访问并处理文件。

27. 如权利要求 23 所述的计算机可读介质，其中步骤 a）包括步骤：

a-1）生成系统安全管理员的公共密钥；

a-2）生成系统安全管理员的保密密钥；和

a-3）生成系统安全管理员的证书。

28. 如权利要求 23 所述的计算机可读介质，其中步骤 e）包括步骤：

e-1）在服务器计算机中生成随机数；

e-2）生成对该随机数的数字签名；

e-3）从存储在安全内核上的系统安全管理员的证书中提取系统安全管理员的公共密钥；

e-4）通过提取的系统安全管理员的公共密钥验证用户的证书；

e-5）提取用户的公共密钥和用户证书中的访问权限；和

e-6）验证对该随机数的数字签名。

29. 如权利要求 23 所述的计算机可读介质，其中步骤 f）包括步骤：

f-1）如果用户是一般用户，则给该用户提供对文件系统的文件系统访问权限；和

f-2）给该用户提供注册/删除权限、文件系统访问设置权限和文件系统访问权限。

30. 如权利要求 24 所述的计算机可读介质，其中步骤 g）包括步骤：

g-1）确定是否选择了用户注册或删除；

g-2）如果选择了用户删除，则删除与将要删除的用户有关的数据；

g-3）如果选择了用户注册，则注册一个用户；

其中的步骤 g-3）包括以下步骤：

g-3-1）提供访问权限给将要注册的用户；

g-3-2）生成将要注册的用户的保密密钥和公共密钥；

g-3-3）生成将要注册的用户的证书；

g-3-4）加密并存储将要注册的用户的保密密钥；和

g-3-5）存储将要注册的用户的证书。

31. 如权利要求 30 所述的计算机可读介质，其中证书是通过加密访问权限和用户的公共密钥生成的。

32. 如权利要求 25 所述的计算机可读介质，其中步骤 h）包括步骤：

h-1）选择一文件；

h-2）选择允许访问该文件的用户；和

h-3）设置对该文件的访问权限为用户的访问权限。

33. 如权利要求 26 所述的计算机可读介质，其中访问并处理文件的步骤 i）包括步骤：

i-1）接收将要访问的文件的名称；

i-2）确定将要访问的文件的访问权限是否等于系统安全管理员的访问权限；

i-3）如果将要访问的文件的访问权限等于系统安全管理员的访问权限，则允许该文件被访问；

i-4）确定将要访问的文件的访问权限是否等于试图对此访问的用户的访问权限；

i-5）如果将要访问的文件的访问权限等于试图对此访问的用户的访问权限，则允许该文件被访问。

说　明　书

基于数字签名证书保护文件系统的方法和装置

发明领域

本发明涉及保护文件系统的方法和装置，更具体地说，涉及一种计算机系统中基于数字签名证书保护文件系统的方法和装置。

背景技术

在常规的计算机系统中，为了保护服务器计算机，使用访问控制方法或一次密码。

使用访问控制方法的计算机系统允许特定的用户仅访问预定的服务或网络地址。也就是说，计算机系统禁止没有访问权限的用户访问预定的服务或预定的网络地址之外的内容。

用来识别用户的通用密码注册以后就一直使用，直到注册另一个密码为止。为了防止恶意的用户蒙混使用该密码，所以使用一次密码。一次密码是指仅使用一次的密码。

但是，由于已经引入恶意的黑客仅通过访问预定的服务或网络地址就能够获取系统安全管理员或普通用户的授权的剽窃方法，对特定服务或网络的访问拦截实际上不可能保护文件系统免受恶意的黑客试图伪造或改变比如主页的文件系统。

各种剽窃技术使一次密码的部分安全功能变得无效。

访问控制方法和一次密码的问题由提供在用户或网络级的应用程序中实施的常规安全技术的计算机操作系统引起。

发明概述

因此，本发明的一个目的是提供一种保护文件系统的方法和装置。

本发明的另一个目的是提供一种安全稳定的计算机系统。

根据本发明的一个方面，提供一种保护计算机中的文件系统的方法，其中具有文件访问权限的用户可以访问计算机中的文件系统，该方法包括步骤：

a）生成系统安全管理员的数字签名密钥和系统安全管理员的证书

（certificate）；b）当在服务器计算机上安装操作系统时，将系统安全管理员的证书存储到安全内核中；c）生成第二数字签名密钥和用户的证书；d）设置文件系统的访问权限；e）当用户试图访问文件系统时，通过基于数字签名的身份验证识别用户；以及f）根据识别结果授予用户对文件的访问权限。

根据本发明的另一方面，提供一种保护计算机中的文件系统的装置，其中具有文件访问权限的用户可以访问计算机中的文件系统，该装置包括：生成系统安全管理员的数字签名密钥和系统安全管理员的证书的部件；当在服务器计算机上安装操作系统时，将系统安全管理员的证书存储到安全内核中的部件；生成用户数字签名密钥和用户的证书的部件；设置文件系统的访问权限的部件；当用户试图访问文件系统时，通过数字签名身份验证的方法识别用户的部件；以及根据识别结果授予用户对文件的访问权限的部件。

附图的简要描述

从下面结合附图对优选实施例的详细描述，本发明的上述和其他目的和特征将变得更加清楚，其中：

图 1 为应用本发明的计算机系统的框图；

图 2 为根据本发明的服务器计算机的详细框图；

图 3 为图 2 的安全内核的详细框图；

图 4 为图 2 的证书存储器的详细框图；

图 5 为图 3 的安全内核中处理安全信息存储器的详细框图；

图 6 为图 3 的安全内核中文件安全信息存储器的详细框图；

图 7 为说明根据本发明用于运行文件保护方法的方法的流程图；

图 8 为说明根据本发明用于在服务器计算机上安装文件保护方法的方法的流程图；

图 9 为说明根据本发明用于运行文件保护方法的方法的流程图；

图 10 为说明根据本发明的基于数字签名的身份验证的流程图；

图 11 为说明根据本发明的注册/删除用户的方法的流程图；

图 12 为说明根据本发明的设置文件访问权限的方法的流程图；和

图 13 为说明处理文件的方法的流程图。

本发明的优选实施例

下面将参照附图详细描述本发明的优选实施例。

图 1 为应用本发明的计算机系统的框图。

该计算机系统包括服务器计算机 110、以及系统安全管理员、到服务器计算机 110 距离遥远的用户和距离较近的用户所用的计算机 120、140 和 150。

每一台计算机 120、140 和 150 具有存储设备，比如软盘 124、144 和 154 以及智能卡 126、146 和 156。服务器计算机 110 和计算机 120、140 和 150 直接或通过计算机网络 130 彼此互连。

在获得基于数字签名的身份验证之后，系统安全管理员管理服务器计算机 110 和服务器计算机 110 的用户。

到服务器计算机 110 距离较近的用户 150 在基于数字签名而被识别后，可以访问部分文件。该部分文件是允许用户访问的。系统安全管理员设置文件的访问权限和用户的访问权限。

到服务器计算机 110 距离遥远的用户 140，在基于由通信生成的数字签名而被识别后，通过计算机网络可以访问允许用户访问的部分文件。

图 2 为根据本发明的服务器计算机的详细框图。

服务器计算机包括多个在用户级、内核级和硬件级中的组件。

服务器计算机的用户级包括证书存储块 212、安全管理模块 214、安全库 216、以及库 218。

安全管理模块 214 生成一对用于生成系统安全管理员或较近/遥远距离处的用户的数字签名值的加密密钥。这对加密密钥包括一个保密密钥和一个公共密钥。另外，安全管理模块 214 基于该加密密钥和数字签名值颁发证书。

服务器计算机的内核级包括系统调用接口块 232、文件子系统 234、处理控制子系统 236、安全内核 238、设备驱动器 240 和硬件控制器 242。

系统调用接口块 232 将用户级中的组件和内核级的组件接口。

安全内核 238 证实数字签名，设置并查询文件的访问权限。另外，安全内核 238 控制文件的访问。

服务器计算机的硬件级包括驱动器控制器、硬盘驱动器、软盘驱动器、智能卡驱动器、通用串行总线（USB）驱动器和网络驱动器。

硬件级中的这些组件对本领域的技术人员是公知的。因此，在本说明书中略去对这些组件的详细描述。

图 3 为图 2 的安全内核的详细框图。

安全内核包括访问权限控制块 302、数字签名验证块 304、访问权限设置/查询块 306、安全规则设置/查询块 308、文件系统访问权限决策块 310、系统安全管理员证书存储器 312、处理安全信息存储器 314、安全规则存储器 316 和文件系统安全信息存储器 318。

与处理过程相关的安全信息存储在处理安全信息存储器 314 中，安全规则信息存储在安全规则存储器 316 中，以及与文件系统有关的安全信息存储在文件系统安全信息存储器 318 中。

访问权限控制块 302 控制访问权限设置/查询块 306、安全规则设置/查询块 308 和文件系统访问权限决策块 310。

访问权限设置/查询块 306 包括处理安全信息设置/查询块 320 和文件系统安全信息设置/查询块 322。如果在访问权限控制块 302 中识别出用户试图访问文件，则在处理安全信息存储器 314 中的信息由处理安全信息设置/查询块 320 设置。

文件系统安全信息设置/查询块 322 设置并查询文件系统安全信息存储器 318。

安全规则设置/查询块 308 设置并查询存储在安全规则存储器 316 中的安全规则。

安全规则设置/查询块 308 与访问权限设置/查询块 306 和文件系统访问权限决策块 310 通信，并根据存储在安全规则存储器 316 中的安全规则提供访问控制所必需的信息。

文件系统访问权限决策块 310 比较存储在处理安全信息存储器 314 中的信息和存储在文件系统安全信息存储器 318 中的文件系统安全信息。文件系统访问权限决策块 310 根据存储在安全规则存储器 316 中的安全规则确定是否将访问权限提供给用户。

图 4 为图 2 的证书存储器的详细框图。

证书存储器 212 包括多个证书。这些证书包括用户身份证明（ID）410、430 和 450、以及用户证书 420、440 和 460。每一个用户身份证明（ID）410 代表拥有各自用户证书 420 的用户。按照来自图 2 的安全管理模块 214 的控制信号添加、删除或搜索该对证书。

用户证书 420 包括系统安全管理员身份证明（SM ID）421、用户身份证

明 422、访问权限身份证明（ID）423、访问有效日期 424、公共密钥 425、颁发时间 426、证书有效日期 427 和数字签名值 428。

系统安全管理员身份证明 421 代表颁发用户证书的系统安全管理员 SM。

用户身份证明 422 代表拥有用户用户证书 420 的用户。

访问权限身份证明（ID）423 代表用户的访问权限。

访问有效日期 424 代表有效时间。在该有效时间用户可以访问文件系统。

公共密钥 425 用于证实用户的数字签名。颁发时间 426 代表颁发用户证书的时间。

数字签名值 428 代表除使用系统安全管理员的保密密钥的数字签名值 428 之外的用户证书的数字符号化（digital-signed）的值。

图 5 为图 3 的安全内核中处理安全信息存储器的详细框图。

在处理安全信息存储器 314 中存储多个处理身份证明（ID）510、系统安全管理员标志 512 和访问权限身份证明（ID）514。处理安全信息存储器 314 搜索将要被访问的处理身份证明 510。在找到该处理 ID 后，根据来自处理安全信息设置/查询块 320、文件系统安全信息设置/查询块 322 或文件系统访问权限决策块 310 的控制信号，处理安全信息存储器 314 设置或查询相应的系统安全管理员标志或访问权限身份证明。

每一个处理 ID 510 代表一个由用户执行的处理。

每一个系统安全管理员标志 512 代表通过其执行一个处理的系统安全管理员。每个访问权限 ID 514 代表对该处理所允许的访问权限。

图 6 为安全内核中文件系统安全信息存储器的详细框图。图 3 中的文件系统安全信息存储器 318 包括文件身份证明（ID）602 和访问权限身份证明（ID）604。根据文件系统安全信息设置/查询块 322 或文件系统访问权限决策块 310 的控制信号，设置或查询相应于文件身份证明（ID）602 的访问权限身份证明（ID）604。

文件身份证明（ID）602 代表用于识别文件的身份证明。访问权限身份证明（ID）604 代表允许访问该文件的用户的访问权限。

图 7 为说明根据本发明用于运行文件保护方法的方法的流程图。

首先，在步骤 702，执行设置系统安全管理员的安装处理。接着，在步骤 704，执行运行处理。在该运行处理中，在用户身份验证之后，执行用户注册/删除处理、文件访问权限设置处理或文件访问处理。然后，在步骤 706，

确定是否终止文件保护方法。如果不终止该方法，则处理继续到步骤 704。如果终止，则结束该方法。

图 8 为说明根据本发明在服务器计算机上安装文件保护方法的方法的流程图。

首先，在步骤 802，服务器计算机生成一对用于系统安全管理员的密钥，一个公共密钥 PK_SM 和一个保密密钥 SK_SM。

在步骤 804，服务器计算机生成用于系统安全管理员的证书。通过系统安全管理员的保密密钥 SK_SM 将系统安全管理员的访问权限 ACID_SM 和系统安全管理员的公共密钥 PK_SM 数字符号化，从而生成用于系统安全管理员的证书。

在步骤 806，系统安全管理员加密他的/她的保密密钥 SK_SM 并将加密的保密密钥存储到存储器设备比如智能卡或软盘上。

在步骤 808，系统安全管理员将他的/她的证书 CERT_SM 存储到存储器设备比如智能卡或软盘上。另外，在步骤 810，系统安全管理员将他的/她的证书 CERT_SM 存储到安全内核 238 中的系统安全管理员证书存储器 312 上。

安装处理终止并返回步骤 704。

图 9 为说明根据本发明用于运行文件保护方法的方法的流程图。

首先，在步骤 902，服务器计算机通过使用基于数字签名的身份验证证实试图访问它的系统安全管理员或用户。在步骤 904，确定身份验证是成功还是失败。

如果身份验证失败，则终止该处理。

如果身份验证成功，则处理前进到步骤 906，加载存储在系统安全管理员证书存储器 312 中的系统安全管理员的证书，并从该系统安全管理员的证书中提取系统安全管理员的访问权限 ACID_SM。然后，处理前进到步骤 908，确定用户的访问权限 ACID_U 是否等于系统安全管理员的访问权限 ACID_SM。

如果用户的访问权限 ACID_U 等于系统安全管理员的访问权限 ACID_SM，则在步骤 910，将系统安全管理员的访问权限应用到用户处理的访问权限 ACID_UP。在步骤 914、916、918 和 920，具有系统安全管理员的访问权限 ACID_SM 的用户处理选择并执行用户注册/删除处理、文件系统访问权限设置处理、以及文件访问处理中的一个。

如果不相等，则在步骤 912，将用户的访问权限 ACID_U 应用到用户处理的访问权限 ACID_UP。在步骤 920，用户处理执行文件访问处理。

然后，处理返回到步骤 706。

图 10 为说明根据本发明的基于数字签名的身份验证处理的流程图。

在步骤 1002，服务器计算机生成一个随机数 R。在步骤 1004，通过使用其保密密钥，用户生成一关于随机数 R 的数字签名值 X。在步骤 1006，服务器计算机加载存储在安全内核 238 的系统安全管理员证书存储器中的系统安全管理员的证书 CERT_SM。在步骤 1008，服务器计算机从系统安全管理员的证书 CERT_SM 中提取系统安全管理员的公共密钥 PK_SM，其中证书 CERT_SM 存储在安全内核上。

在步骤 1010，安全内核 238 证实用户的证书 CERT_U。接着，在步骤 1012，确定证实结果为成功还是失败。如果证实结果为失败，则该处理存储证实结果为失败并终止。

如果证实结果为成功，则在步骤 1014，安全内核从用户的证书 CERT_U 中提取公共密钥 PK_U 和用户的访问权限 ACID_U。在提取公共密钥和客户机用户的访问权限之后，在步骤 1016，安全内核证实对随机数 R 的数字签名值 X。如果身份验证结果为成功，则该处理存储身份验证结果为成功并将用户的访问权限 ACID_U 返回给步骤 904，以便在步骤 908 中使用。

图 11 为说明根据本发明的用户注册/删除处理的流程图。

首先，在步骤 1102，确定用户处理的访问权限 ACID_UP 是否等于系统安全管理员的访问权限 ACID_SM。如果用户处理的访问权限 ACID_UP 不等于系统安全管理员的访问权限 ACID_SM，则处理终止并返回。

如果用户处理的访问权限 ACID_UP 等于系统安全管理员的访问权限 ACID_SM，则处理前进到步骤 1104，选择用户注册处理或用户删除处理。

如果选择用户删除处理，则在步骤 1106，具有系统安全管理员的访问权限的用户处理将注册的用户删除。

如果选择用户注册处理，则在步骤 1110，具有系统安全管理员的访问权限的用户处理将访问权限指定给一个新的用户。在步骤 1112，该用户处理为新的用户生成公共密钥 PK_U 和保密密钥 SK_U。

在步骤 1114，系统安全管理员使用其保密密钥加密该用于新用户的访问权限和公共密钥，从而为该新用户生成一个证书 CERT_U。在步骤 1116，该

新用户加密其保密密钥并将该加密的保密密钥存储在存储器设备比如智能卡或软盘上。在步骤 1118，新用户将其证书 CERT_U 存储到存储器上。接着，在步骤 1120，确定是否终止该处理。如果终止该处理，则处理返回。如果不终止，则处理前进到步骤 1104，选择用户注册处理或用户删除处理。

图 12 为说明根据本发明的文件访问权限设置处理流程图。

首先，在步骤 1202，确定用户处理的访问权限 ACID_UP 是否等于系统安全管理员的访问权限 ACID_SM。如果用户处理的访问权限 ACID_UP 等于系统安全管理员的访问权限 ACID_SM，则在步骤 1204，系统安全管理员选择一个要被设置访问权限的文件。如果不相等，则处理终止。

在步骤 1206，系统安全管理员选择允许访问该文件的用户。在步骤 1208，安全内核将在步骤 1204 选择的文件的访问权限 ACID_F 设置为在步骤 1206 选择的用户的访问权限 ACID_U。接着，在步骤 1210，确定是否终止处理。如果服务器计算机选择终止，则处理终止。否则，处理前进到步骤 1204。

图 13 为说明处理文件的方法的流程图。

在步骤 1302，安全内核获取将要被访问的文件。在步骤 1304，安全内核将试图访问该文件的用户处理的访问权限 ACID_UP 与系统安全管理员的访问权限 ACID_SM 相比较。

如果用户处理的访问权限 ACID_UP 等于系统安全管理员的访问权限 ACID_SM，则在步骤 1306，服务器计算机允许用户处理访问该文件。接着，确定是否终止处理。如果服务器计算机选择终止，则处理终止。否则，处理前进到步骤 1302。

如果客户机用户处理的访问权限不等于系统安全管理员的访问权限，则处理前进到步骤 1308，在步骤 1308，确定用户处理的访问权限 ACID_UP 是否等于用户的访问权限 ACID_U。如果不相等，则处理终止。

如果用户处理的访问权限 ACID_UP 等于用户的访问权限 ACID_U，在步骤 1310，确定用户处理的访问权限 ACID_UP 是否等于文件 F 的访问权限 ACID_F。如果不相等，则处理终止。

如果用户处理的访问权限 ACID_UP 等于文件 F 的访问权限 ACID_F，则在步骤 1312，服务器计算机允许该用户处理访问该文件。接着，确定是否终止处理。如果服务器计算机选择终止，则处理终止。否则，处理前进到步骤 1302。

根据本发明的文件保护系统在系统安装处理时将系统安全管理员的证书存储到内核级的安全内核上。另外，不在用户级而在内核级中执行基于身份验证的数字签名、文件访问权限设置处理、以及文件访问处理。从而，该文件保护系统能够从根本上防止文件系统被伪造或改变。

因此，根据本发明的文件保护系统提供一种稳定而且可靠的文件系统。比如，根据本发明的文件保护系统能够保护运行网页的网络服务器系统被攻击。

尽管出于说明目的公开了本发明的优选实施例，但是本领域的技术人员应该理解，在不脱离如所附权利要求中声明的本发明的范围和构思的情况下，可以对本发明进行各种修改、添加和替换。

说 明 书 附 图

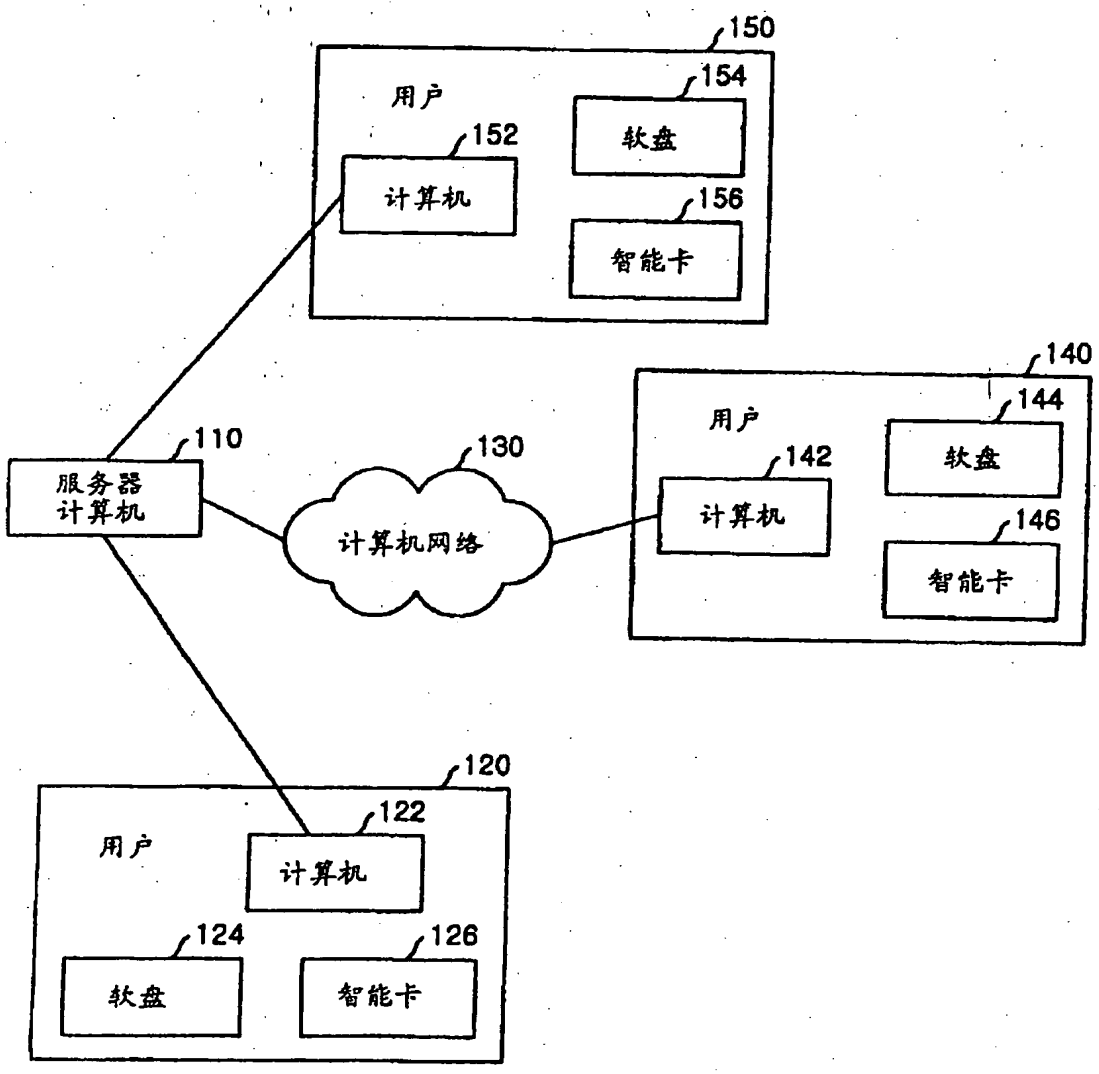

150
用户
154
软盘
152
计算机
156
智能卡
140
用户
144
软盘
142
计算机
146
智能卡
110
服务器
计算机
130
计算机网络
120
用户
122
计算机
124
软盘
126
智能卡

图 1

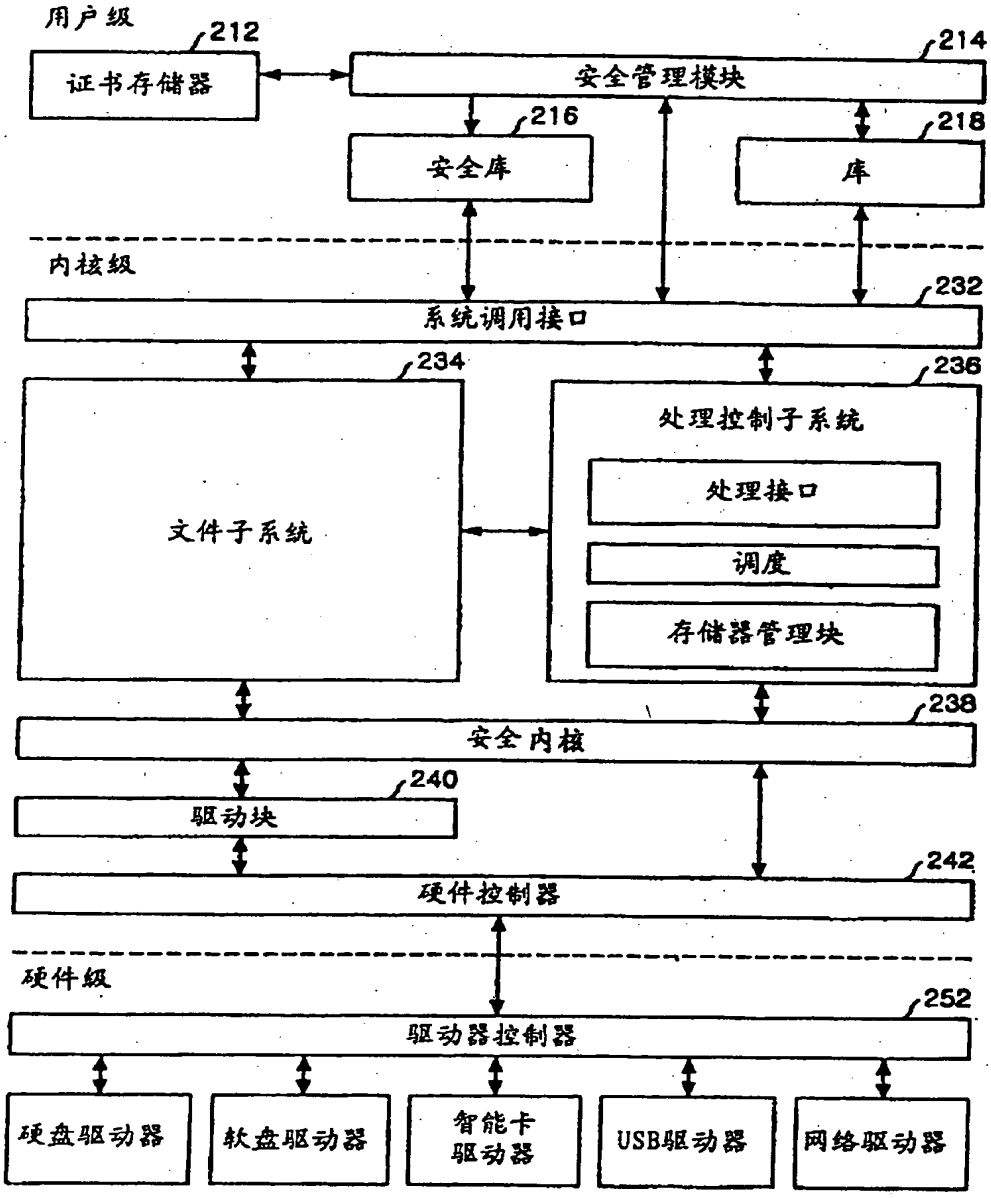

用户级
212
证书存储器
214
安全管理模块
216
安全库
218
库
内核级
232
系统调用接口
234
文件子系统
236
处理控制子系统
处理接口
调度
存储器管理块
238
安全内核
240
驱动块
242
硬件控制器
硬件级
252
驱动器控制器
硬盘驱动器
软盘驱动器
智能卡
驱动器
USB驱动器
网络驱动器

图 2

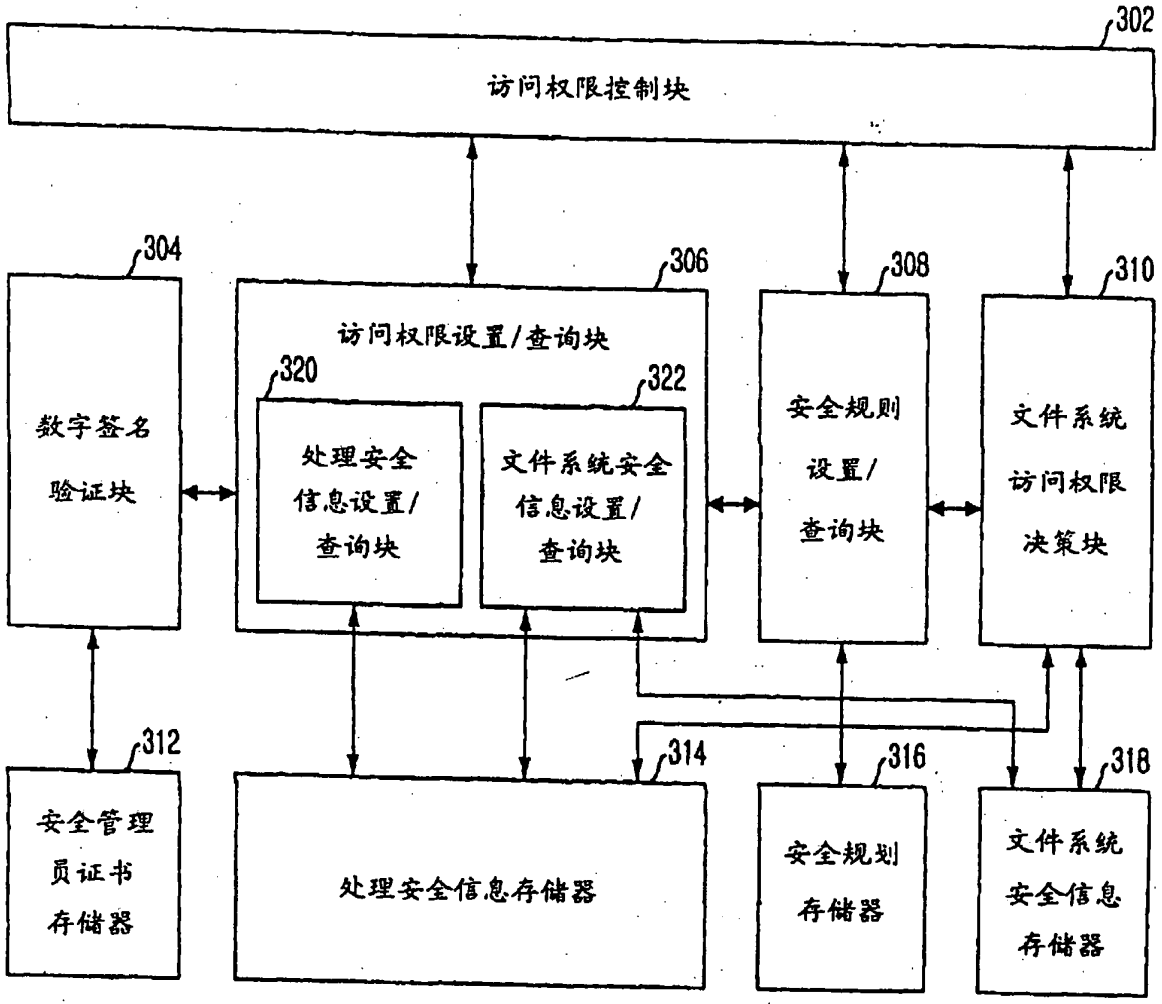

302
访问权限控制块
304
数字签名验证块
306
访问权限设置/查询块
320
处理安全信息设置/查询块
322
文件系统安全信息设置/查询块
308
安全规则设置/查询块
310
文件系统访问权限决策块
312
安全管理员证书存储器
314
处理安全信息存储器
316
安全规则存储器
318
文件系统安全信息存储器

图 3

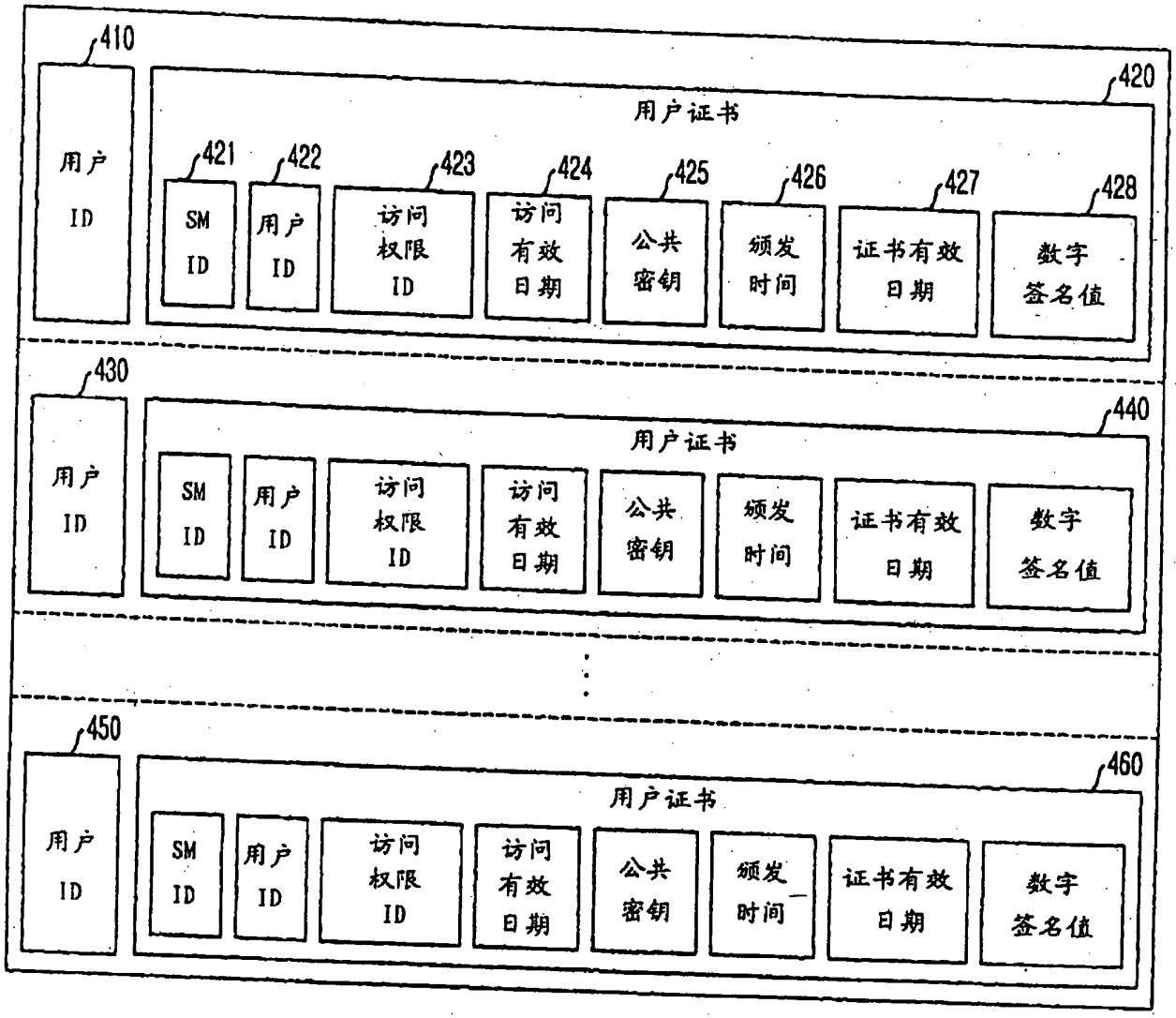

410
用户ID
420
用户证书
421
SM ID
422
用户ID
423
访问权限ID
424
访问有效日期
425
公共密钥
426
颁发时间
427
证书有效日期
428
数字签名值
430
用户ID
440
用户证书
SM ID
用户ID
访问权限ID
访问有效日期
公共密钥
颁发时间
证书有效日期
数字签名值
450
用户ID
460
用户证书
SM ID
用户ID
访问权限ID
访问有效日期
公共密钥
颁发时间
证书有效日期
数字签名值

图 4

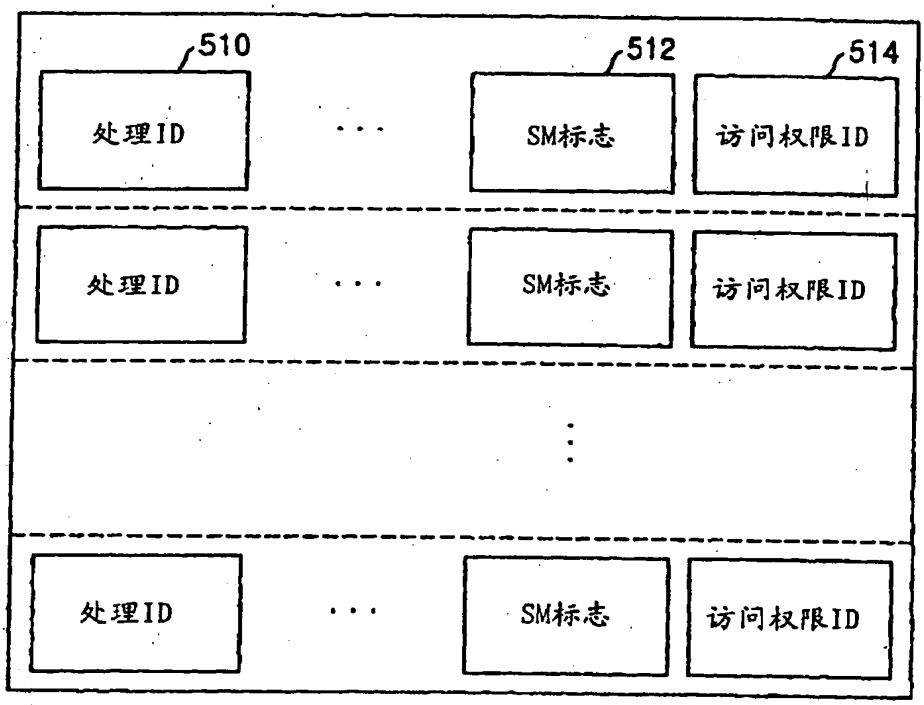

510
512
514
处理ID
SM标志
访问权限ID
处理ID
SM标志
访问权限ID
处理ID
SM标志
访问权限ID

图 5

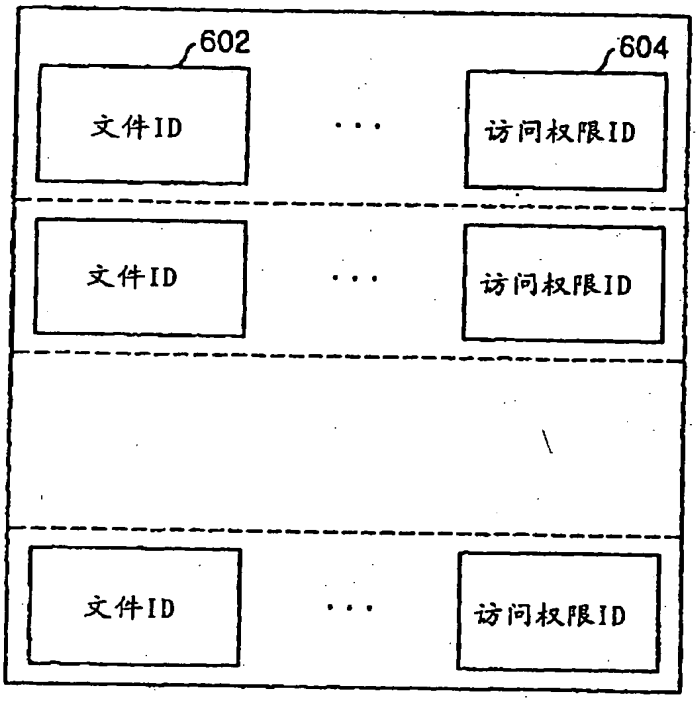


图 6

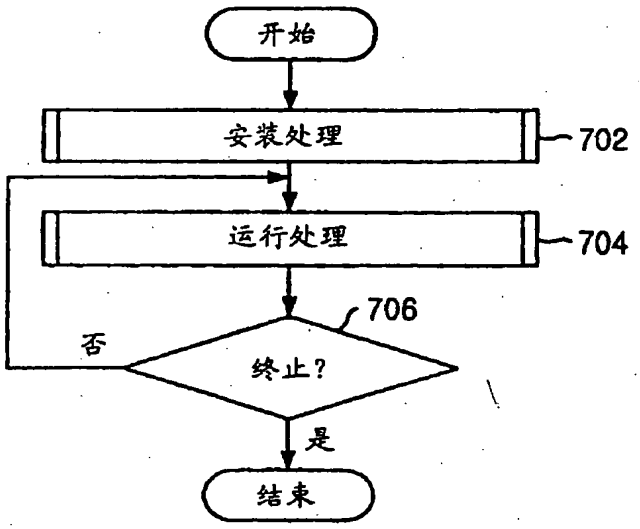


图 7

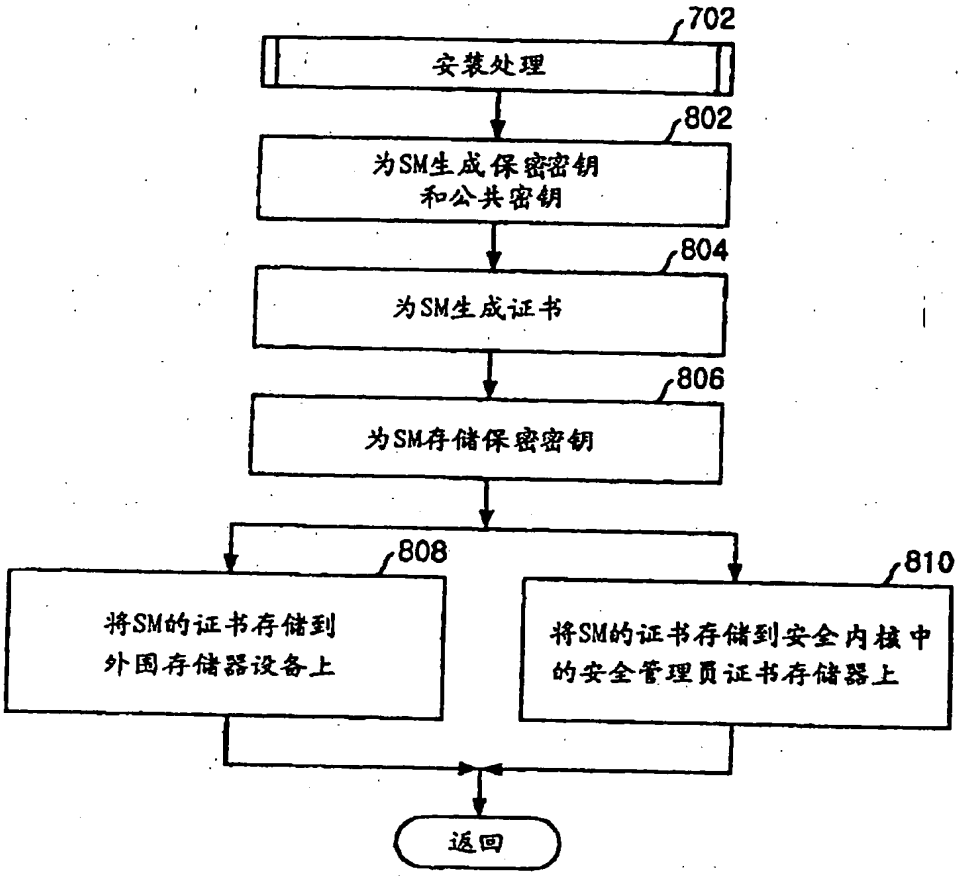

702
安装处理
802
为SM生成保密密钥
和公共密钥
804
为SM生成证书
806
为SM存储保密密钥
808
将SM的证书存储到
外围存储器设备上
810
将SM的证书存储到安全内核中
的安全管理员证书存储器上
返回

图 8

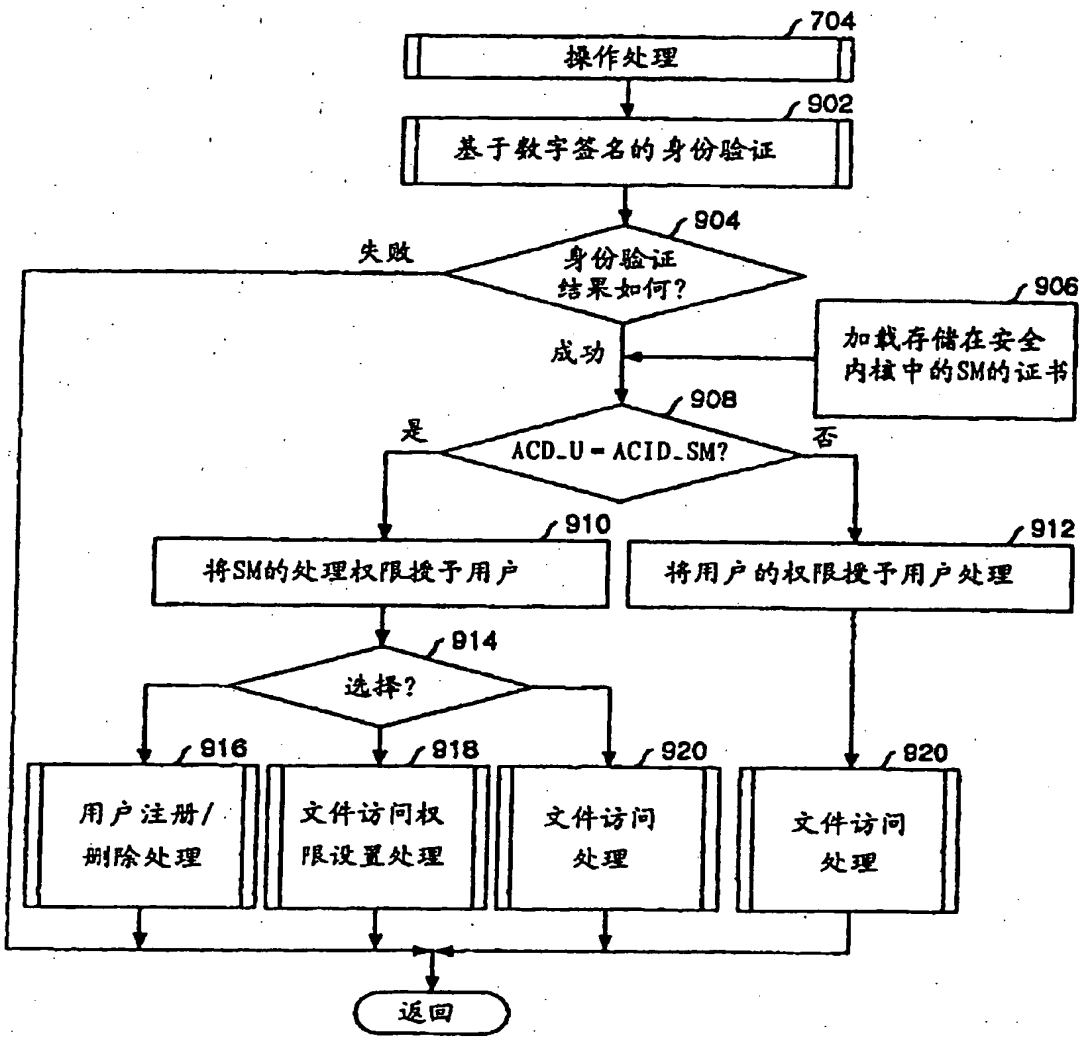

704
操作处理
902
基于数字签名的身份验证
904
身份验证
结果如何?
失败
成功
906
加载存储在安全
内核中的SM的证书
908
ACD_U = ACID_SM?
是
否
910
将SM的处理权限授予用户
912
将用户的权限授予用户处理
914
选择?
916
用户注册/
删除处理
918
文件访问权
限设置处理
920
文件访问
处理
920
文件访问
处理
返回

图 9

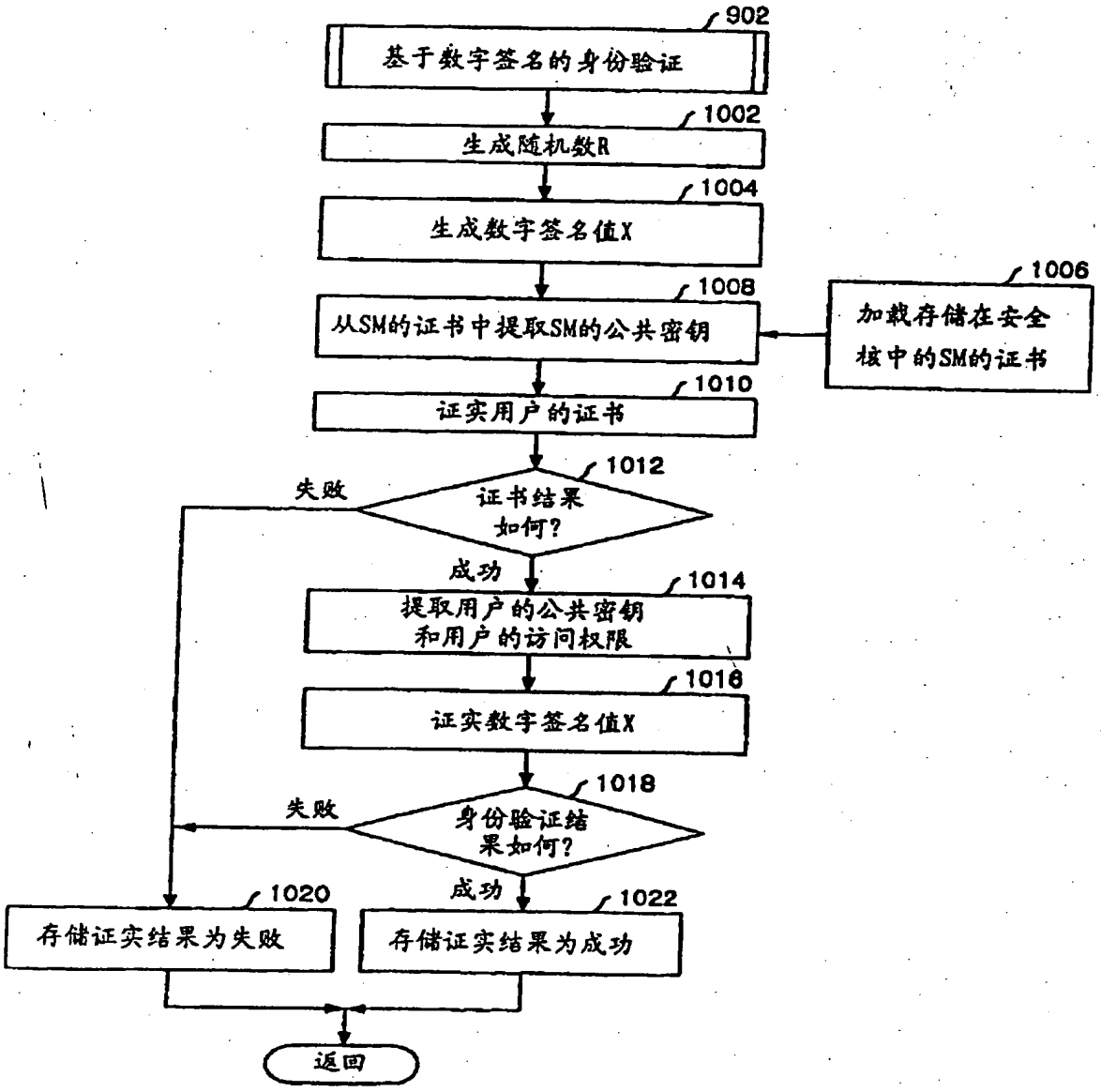

902
基于数字签名的身份验证
1002
生成随机数R
1004
生成数字签名值X
1006
加载存储在安全核中的SM的证书
1008
从SM的证书中提取SM的公共密钥
1010
证实用户的证书
1012
证书结果如何?
失败
成功
1014
提取用户的公共密钥和用户的访问权限
1016
证实数字签名值X
1018
身份验证结果如何?
失败
成功
1020
存储证实结果为失败
1022
存储证实结果为成功
返回

图 10

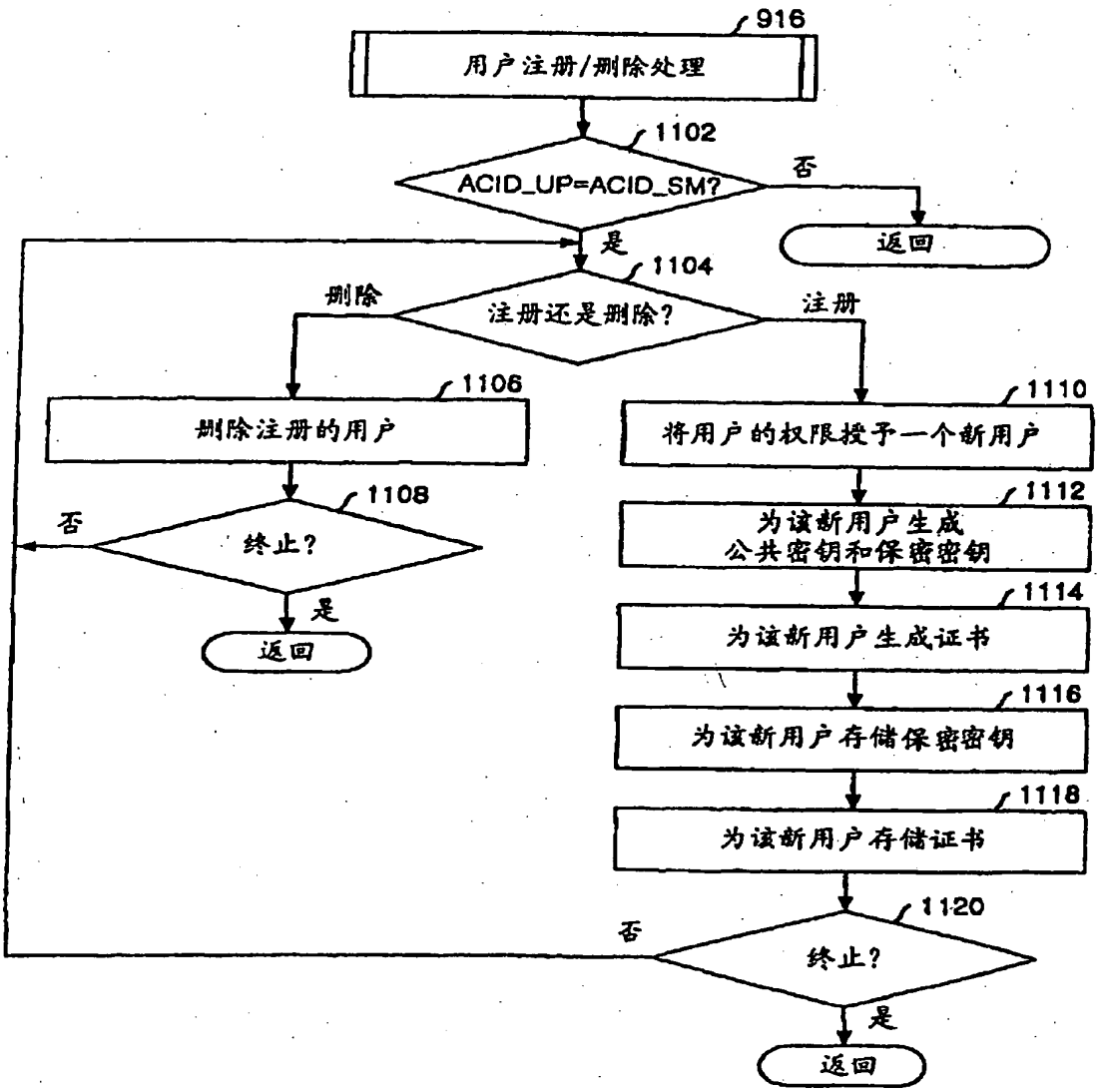

916
用户注册/删除处理
1102
ACID_UP=ACID_SM?
否
返回
是
1104
删除
注册还是删除?
注册
1106
删除注册的用户
1108
否
终止?
是
返回
1110
将用户的权限授予一个新用户
1112
为该新用户生成
公共密钥和保密密钥
1114
为该新用户生成证书
1116
为该新用户存储保密密钥
1118
为该新用户存储证书
1120
否
终止?
是
返回

图 11

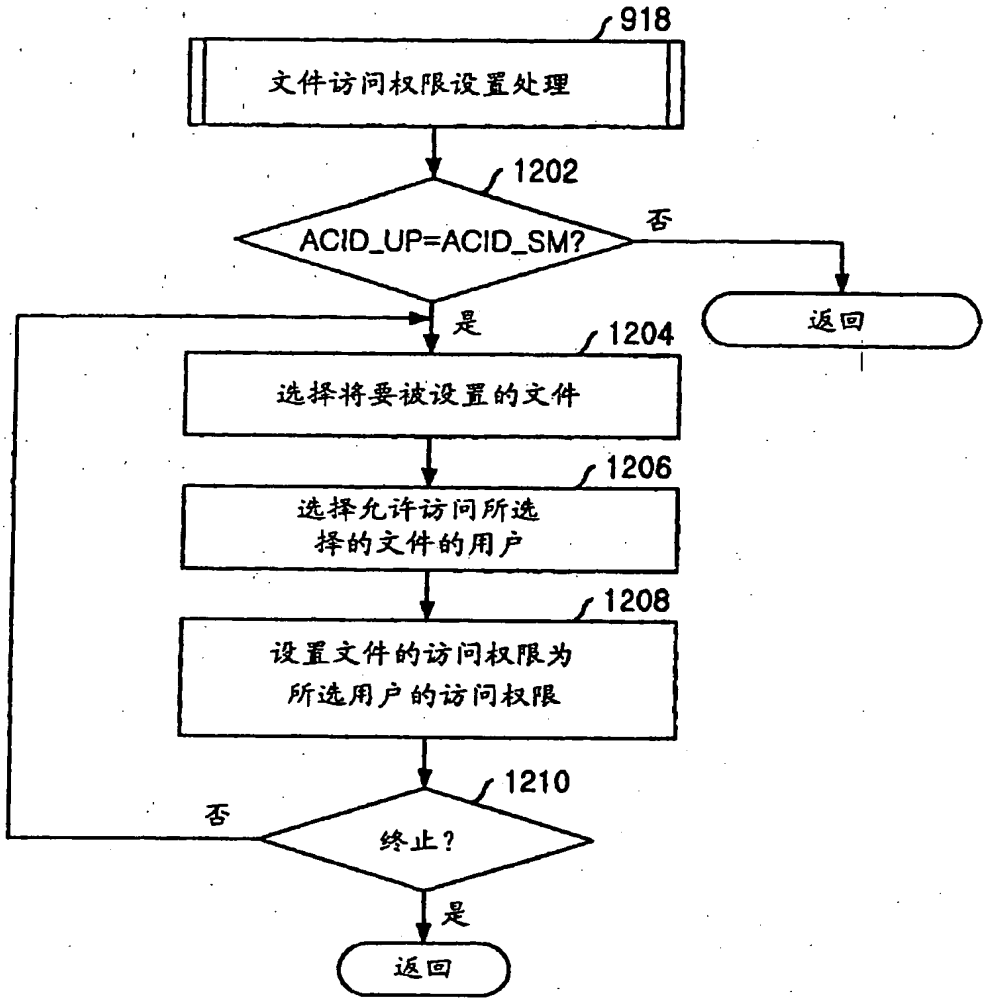

918
文件访问权限设置处理
1202
ACID_UP=ACID_SM?
否
返回
是
1204
选择将要被设置的文件
1206
选择允许访问所选
择的文件的用户
1208
设置文件的访问权限为
所选用户的访问权限
1210
否
终止?
是
返回

图 12

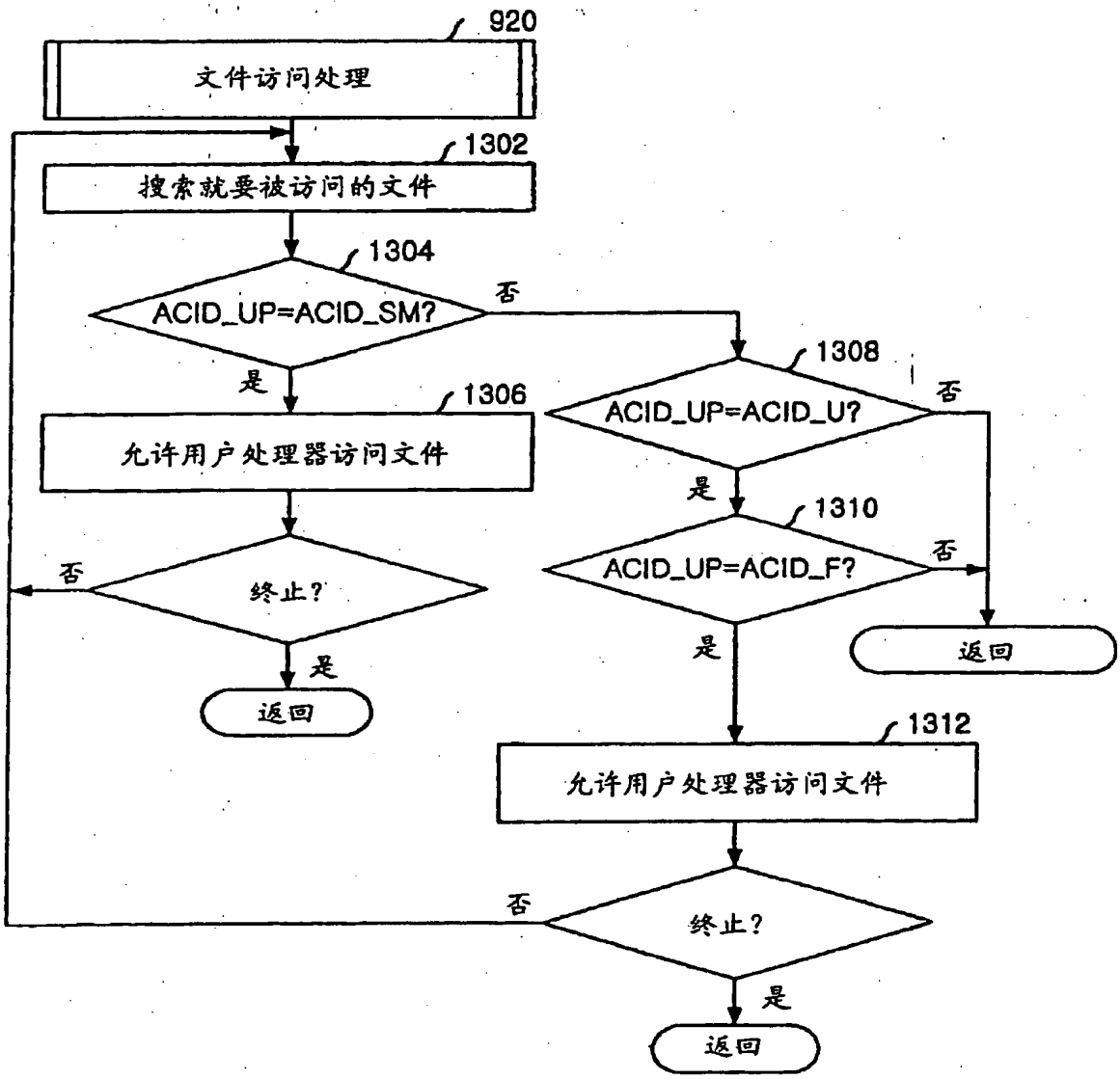

920
文件访问处理
1302
搜索就要被访问的文件
1304
ACID_UP=ACID_SM?
否
是
1306
允许用户处理器访问文件
否
终止?
是
返回
1308
ACID_UP=ACID_U?
否
是
1310
ACID_UP=ACID_F?
否
返回
是
1312
允许用户处理器访问文件
否
终止?
是
返回

图 13